ABSTRACT

Disclosed is a processor having a normal execution mode and a secure execution mode to create a secure execution environment. A secure virtual machine monitor (SVMM) implements the secure execution environment in which a plurality of separate virtual machines are created that operate simultaneously and separately from one another including at least a first virtual machine to implement trusted guest software in a protected memory area and a second virtual machine to implement a non-trusted guest operating system (OS) simultaneously in a non-protected memory area. Responsive to a command to tear down the secure execution environment, the SVMM causes the processor to exit out of the secure execution mode, tears down the secure execution environment, and instructs the non-trusted guest OS to resume control in the normal execution mode.